What is claimed is:

[Claim 1] A method for blocking submission of online forms presented by a browsing program comprising the steps of:

- detecting form data before a form is submitted to a target site;
- accessing said form data;
- detecting sensitive form fields within said form data;
- analyzing URL and certificate of said target site against security criteria to generate an alert code;
- matching said alert code with blocking criteria to generate a match condition;
- blocking submission of said form to said target site if said match condition is generated.

[Claim 2] The method of claim one wherein the step of detecting sensitive form data further includes:

- receiving a notification message from said browsing program that form data is about to be submitted;
- receiving a URL of said target site together with said notification message.

[Claim 3] The method of claim two wherein the step of analyzing said target site further includes checking for at least one of the following attributes:

- site server being listed in saved sites database;
- secure communication protocol in the URL of target site and a valid site server certificate.

[Claim 4] The method of claim three wherein blocking criteria are determined by a user and the steps of matching alert codes with blocking criteria further include:

- inputting by said user a list of alert codes which should cause an alert;
- generating a physical alert if any of analysis results match at least one entry in said list;

- presenting to said user said physical alert;
- accepting enable/disable submission input from said user;
- generating a match condition if a disable input is received from said user.

[Claim 5] The method of claim three wherein preset security triggers are determined by an automated policy and the steps of matching analysis results with blocking criteria further include:

- comparing generated alert code with rules specified in an a policy;
- generating a match condition if at least one policy rule matches said alert code.

[Claim 6] The method of claim one wherein the step of detecting form data further includes:

- detecting a network login dialog window containing at least a password field;
- retrieving a URL of said target site from a browsing program.

[Claim 7] The methods of claims six wherein the step of analyzing said target site further includes checking for at least one of the following attributes:

- site server being listed in saved sites database;
- secure communication protocol in the URL of target site and a valid site server certificate.

[Claim 8] The method of claim seven wherein blocking criteria are determined by a user and the steps of matching alert codes with blocking criteria further include:

- inputting by said user a list of alert codes which should cause an alert;
- generating a physical alert if any of analysis results match at least one entry in said list;
- presenting to said user said physical alert;
- accepting enable/disable submission input from said user;
- generating a match condition if a disable input is received from said user.

[Claim 9] The method of claim seven wherein preset security triggers are determined by an automated policy and the steps of matching analysis results with blocking criteria further include:

- comparing generated alert code with rules specified in an a policy;
- generating a match condition if at least one policy rule matches said alert code.

[Claim 10] A system for blocking submission of online forms, comprising a computing device with access to a network, a first browsing program adapted to be executed on said device and a second monitoring program adapted to be executed on said device configured to:

- accept notifications from said browsing program before a form is submitted to a target site;
- access form data in said browsing program and detect form fields of a sensitive nature;
- retrieve from said browsing program a URL of said target site;
- analyze URL and certificate of said target site against security criteria to generate an alert code;
- match said alert code with blocking criteria to generate a match condition;
- block submission of said online form to said target site if said match condition is generated.

[Claim 11] The system of claim ten wherein analyzing URL and certificate constitutes checking for at least one of the following attributes:

- site server being listed in saved sites database;
- secure communication protocol in the URL of target site and a valid site server certificate.

[Claim 12] The system of claim eleven where said monitoring program is part of a password management program adapted to be executed on said device.

[Claim 13] The system of claim eleven wherein said monitoring program is an integrated part of said browsing program.